RENOBO EMPRESA DE RENOVACIÓN Y DESARROLLO URBANO DE BOGOTÁ

Política para la Administración de Riesgos

TABLA DE CONTENIDO

Política para la Administración de Riesgos

1. COMPROMISO DE LA EMPRESA FRENTE A LA GESTIÓN DE RIESGOS

La Alta Dirección se compromete a gestionar de manera efectiva los riesgos que pueden afectar el logro de la misión, objetivos estratégicos, planes, programas, proyectos y procesos, a través de la aplicación de la **Política para la Administración de Riesgos**, que brinda directrices para identificar, determinar y aplicar las acciones oportunas y efectivas de control, que contribuyen a evitar su materialización y en caso de ello, definir actuaciones de contingencia inmediatas que permitan mitigar las posibles consecuencias con el fin de mantener los niveles de riesgo aceptables.

La empresa adopta esta política con un enfoque preventivo para garantizar razonablemente el cumplimiento de sus objetivos y mejoramiento de la prestación de los servicios a la ciudadanía, el cual incluye los lineamientos que orientan las acciones necesarias para gestionar los riesgos a los cuales está expuesta la Empresa, de acuerdo con lo establecido en la *Guía para la administración del riesgo y el diseño de controles en entidades públicas* del DAFP del 2022[1].

Finalmente, es importante precisar, que esta política está incluida y articulada con la **Política Integral de Gestión**, que recoge lineamientos de varios modelos de gestión que la requieren, para facilitar y garantizar la implementación de este requerimiento de manera coherente, organizada y articulada.

[1] Si bien esta versión incorpora el Riesgo Fiscal, su implementación en la Empresa se llevará a cabo de manera progresiva, por lo que en esta versión de la política no se incluyen lineamientos relacionados con este tipo de riesgo.

Política para la Administración de Riesgos

2. OBJETIVO

Definir los lineamientos para identificar, analizar, valorar y determinar el tratamiento a los riesgos asociados con los objetivos institucionales y de los procesos con el fin de aportar a su cumplimiento y articular este documento con las demás políticas y planes institucionales de modo que se contribuya con el logro razonable de los propósitos y metas institucionales.

3. ALCANCE

Esta política aplica para todos los procesos, proyectos y planes de la Empresa.

Hace parte integral de esta Política todos los mecanismos, metodologías e instrumentos diseñados para su implementación.

4. MARCO NORMATIVO

Ver Normograma de la Empresa de Renovación y Desarrollo Urbano de Bogotá.

5. DEFINICIONES[2]

Activo: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

Alta Dirección: Se considera Alta Dirección a los directivos con cargo más alto en la empresa, Representante Legal y su equipo Directivo. Los miembros de la Alta Dirección poseen autoridad, recursos y poder de decisión sobre los cambios organizacionales, así mismo, guían los objetivos y estrategias de la Empresa.

Amenaza: Situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

[2] Guía para la administración del riesgo y el diseño de controles en entidades públicas. DAFP. 2022.

Política para la Administración de Riesgos

Análisis del riesgo: Proceso para comprender la naturaleza del riesgo y establecer su probabilidad e impacto.

Apetito del riesgo: Es el nivel de riesgo que la entidad puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

Capacidad de riesgo: Es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual la Alta Dirección considera que no sería posible el logro de los objetivos de la entidad.

Causa: Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

Causa inmediata: Circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.

Causa raíz: Es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, constituye la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo puede existir más de una causa o subcausas que pueden ser analizadas.

Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados.

Consecuencia: Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Control: Medida que permite reducir o mitigar un riesgo

Disponibilidad: Propiedad de ser accesible y utilizable a demanda por una entidad.

Factores de Riesgo: Son las fuentes generadoras de riesgos.

Financiación del terrorismo: Es el conjunto de actividades encaminadas a canalizar recursos lícitos o ilícitos para promover, sufragar o patrocinar individuos, grupos o actividades terroristas.

Impacto: Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Incidente: Es un evento no planificado que interrumpe el curso normal de las operaciones y puede causar daños, pérdidas o afectar negativamente a las personas, los activos, el medio ambiente o la reputación de una organización.

Integridad: Propiedad de exactitud y completitud.

Lavado de activos: Es la modalidad mediante la cual organizaciones criminales buscan dar apariencia de legalidad a los recursos que obtienen de sus actividades ilícitas, mediante la incorporación de estos en el circuito económico legal. A través de esta actividad, las bandas delincuenciales consiguen hacer uso de estos activos sin poner en peligro su reinversión en nuevas actividades ilícitas o lícitas.[3]

Líder o responsable de proceso: Encargado de velar por el cumplimiento de los objetivos, la ejecución de las actividades y gestión de todos los temas asociados con el proceso asignado. Respecto a la gestión de riesgos, debe estar involucrado en las actividades de identificación, valoración e implementación de la metodología de administración de riesgos, asegurando en todo momento que se dispone de las métricas necesarias para su correcta monitorización, evaluación y eventual mejora.

Materialización del riesgo: Situación que nos demuestra que el riesgo ya es una falla o problema real, es decir, cuando ya existe un problema o falla en la gestión que impactó en la operación o sostenibilidad de la empresa.

Nivel de riesgo: Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos.

Mapa de riesgos: Documento que permite organizar la información sobre la gestión del riesgo de la Empresa y visualizar su impacto, con la finalidad de establecer las estrategias adecuadas para su manejo.

Plan de contingencia[4]: Procedimientos documentados que guían y orientan a las organizaciones para responder, recuperar, reanudar y restaurar la operación a un nivel predefinido de operación una vez presentada o tras la interrupción para garantizar la

[3] Lo que debe saber sobre el Lavado de Activos y la Financiación del Terrorismo. Documentos UIAF. 2014.
[4] Guía para la preparación de las TIC para la continuidad del negocio emitida por el Ministerio TIC.

continuidad de las funciones críticas del negocio. Se enmarca dentro del Plan de Continuidad de Negocio y se consideraría un control correctivo.

Probabilidad: Se entiende como la posibilidad de ocurrencia del riesgo. La probabilidad de ocurrencia estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Puntos de riesgo: Son actividades dentro del flujo del proceso donde existe evidencia o se tienen indicios de que pueden ocurrir eventos de riesgo operativo y deben mantenerse bajo control para asegurar que el proceso cumpla con su objetivo.

Riesgo: Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos. Las consecuencias pueden ser positivas o negativas.

Riesgo ambiental: Se entiende como los daños o pérdidas potenciales que pueden presentarse debido a los eventos físicos peligrosos de origen natural, socio-natural tecnológico, biosanitario o humano no intencional, en un período de tiempo específico y que son determinados por la vulnerabilidad de los elementos expuestos; por consiguiente, el riesgo de desastres se deriva de la combinación de la amenaza y la vulnerabilidad.[5]

Riesgo de corrupción: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Riesgo de gestión: Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.

Riesgo de Lavado de Activos y Financiación del Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva LA/FT/FPADM: Se define como la posibilidad de pérdida o daño que puede sufrir una entidad por su propensión a ser utilizada directa o indirectamente a través de sus operaciones como instrumento para el lavado de activos, canalización de recursos hacia la realización de actividades terroristas

[5] Ley 1523 de 2012

y/o financiación de armas de destrucción masiva, o cuando se pretenda el ocultamiento de activos provenientes de dichas actividades.[6]

Riesgo de proyectos: Evento o condición incierta que, en caso de que ocurra, tiene un efecto positivo o negativo sobre al menos un objetivo del proyecto, ya sea tiempo, costo, alcance o calidad.

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Riesgo de seguridad y salud en el trabajo: Combinación de la probabilidad de que ocurra un evento o exposición peligrosa relacionada con el trabajo y la severidad de la lesión y deterioro de la salud que puede causar el evento o exposición.[7]

Riesgo inherente: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto, nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.

Riesgo residual: Resultado de aplicar la efectividad de los controles al riesgo inherente. Es el riesgo que permanece tras implementar las medidas efectivas para reducir el riesgo inherente.

SARLAFT: Sistema de Administración de Lavado de Activos y Financiación del Terrorismo. Es un mecanismo que permite a las entidades prevenir la pérdida o daño que pueden sufrir por su propensión a ser utilizadas como instrumento para el lavado de activos y/o canalización de recursos hacia la realización de actividades terroristas, por sus clientes o usuarios.

Tolerancia al riesgo: Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.

Vulnerabilidad: Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas.

[6] Documento Técnico. Adaptación de Medidas de Prevención y mitigación del riesgo del lavado de activos, financiación del terrorismo en las entidades del distrito capital. Diciembre de 2022
[7] NTC ISO 45001:2018.

6. ALINEACIÓN ESTRATÉGICA

Esta política se encuentra alineada y aporta a logro de los pilares definidos en el Plan Estratégico “Revitalización Urbana 2024 - 2027”, específicamente con el tercer pilar “Excelencia operacional”.

7. DESARROLLO DE LA POLÍTICA

7.1 TIPOS DE RIESGO

Los tipos de riesgos que se deben gestionar en la Empresa, así como el documento que describe los pasos a seguir para su identificación, análisis, evaluación, y establecimiento de las estrategias para su tratamiento y monitoreo, se relacionan a continuación[8]:

Tipo de riesgo		Compromiso de la Empresa frente al tipo de riesgo	Documento asociado
	Gestión	Definir e implementar acciones tendientes a reducir los eventos negativos o potenciales negativos que llegasen a materializarse en los procesos.	GI-05 Guía para la administración de riesgos
	Corrupción	Gestionar eventos asociados a la posibilidad de que, por acción u omisión se use el poder para desviar la gestión de lo público hacia un beneficio privado.	GI-05 Guía para la administración de riesgos
	Seguridad de la información	Gestionar la posibilidad de que ciertas amenazas puedan explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

[8] Respecto a riesgos fiscales, su implementación se llevará a cabo de manera progresiva por lo que no se contemplan en esta versión de la política.

Tipo de riesgo		Compromiso de la Empresa frente al tipo de riesgo	Documento asociado
	Seguridad y salud en el trabajo	Prevenir los peligros y establecer controles frente a los riesgos de Seguridad y Salud en el trabajo.	MN-06 Manual del Sistema de Gestión de Seguridad y Salud en el Trabajo – SG-SST
	Ambientales (aspectos e impactos)	Identificar, valorar y establecer acciones frente a los aspectos e impactos ambientales de la empresa.	PD-30 Identificación y valoración de aspectos e impactos ambientales
	Lavado de activos y financiación del terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva LA/FT/FPADM	Gestionar los riesgos de Lavado de Activos y Financiación del Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva LA/FT/FPADM.	Por definir
	De proyectos	Identificar, evaluar y hacer seguimiento a los riesgos de proyectos y acciones de tratamiento, para minimizar el impacto que se produzca de la posible materialización en desarrollo de estos.	GI-49 Guía de Gestión Integral de Proyectos

Nota: Los íconos podrán utilizarse en el desarrollo del documento para identificar la información aplicable.

7.2 PAUTAS GENERALES SOBRE LOS RIESGOS

A continuación, se describen las pautas generales para gestionar, hacer seguimiento y evaluar los riesgos institucionales de la Empresa, articulándola con las demás políticas y planes existentes para contribuir al desempeño y asegurar razonablemente el logro de los propósitos y metas institucionales.

7.2.1 Niveles de aceptación del riesgo

De acuerdo con lo establecido en la *Guía para la administración del riesgo y el diseño de controles en entidades públicas* del DAFP del 2022, se definen 4 zonas de severidad en la matriz de calor, a través de la combinación entre la probabilidad y el impacto:

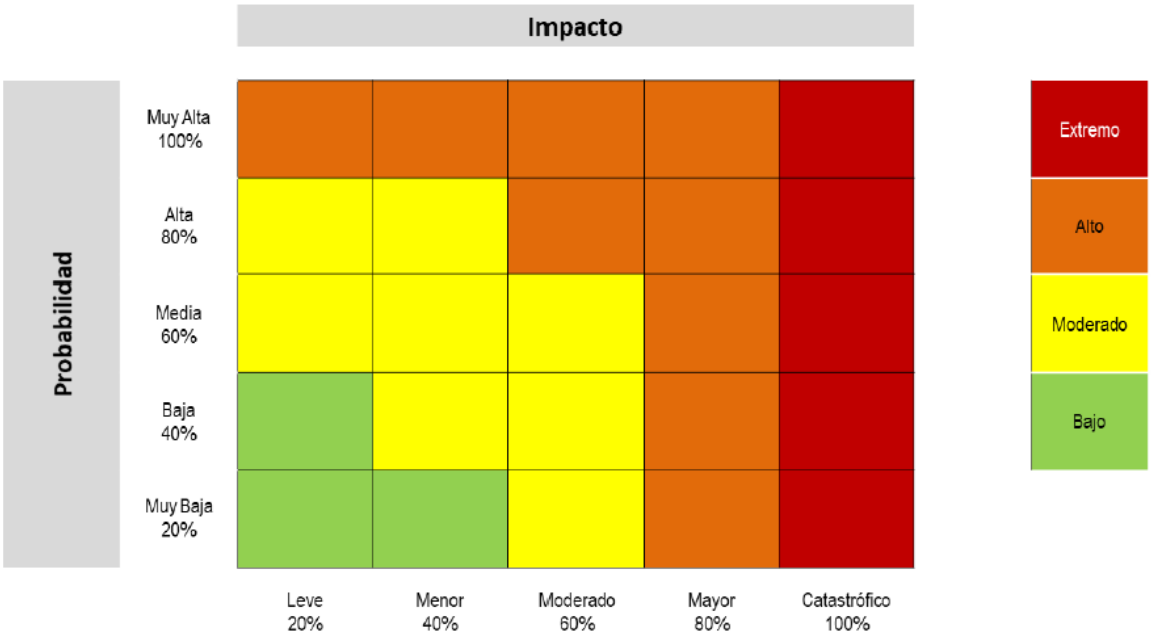


Figura 1. Matriz de calor (niveles de severidad del riesgo)
Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. DAFP 2022.

De acuerdo con lo anterior, el nivel de riesgo que la empresa puede aceptar, que podría permitir el logro de los objetivos institucionales se describe a continuación.

- Para los riesgos que se encuentren en **zona de riesgo baja**, la Empresa está dispuesta a **aceptar** el riesgo, conociendo los efectos de su posible materialización y para los cuales se deben establecer los controles, no se requiere la definición de acciones de tratamiento, y se deben monitorear conforme a la periodicidad establecida.

- Para los riesgos calificados de **zona moderada a extrema**, se deben establecer los controles y acciones de tratamiento que los mitiguen o reduzcan y se deben monitorear conforme a la periodicidad establecida.

- Los riesgos asociados a posibles actos de corrupción **no admiten aceptación** y se deben definir los lineamientos para su tratamiento. De igual manera, se deben monitorear conforme a la periodicidad establecida.

- Cuando sea muy difícil para la empresa reducir el riesgo a un nivel aceptable o se carece de conocimientos necesarios para gestionarlo, éste puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia. Los dos principales métodos de compartir o transferir parte del riesgo son: seguros y tercerización. Estos mecanismos de transferencia de riesgos deberán estar formalizados a través de un acuerdo contractual. No aplica para riesgos de corrupción.

- Los Líderes de Proceso ante la materialización de los riesgos que impliquen la interrupción de las operaciones deben reportarlo a las instancias de control internas y externas correspondientes con el tipo de riesgo e implementar los planes de contingencia y/o continuidad, correspondientes. Este reporte se debe realizar a través del formulario disponible en la intranet para tal fin.

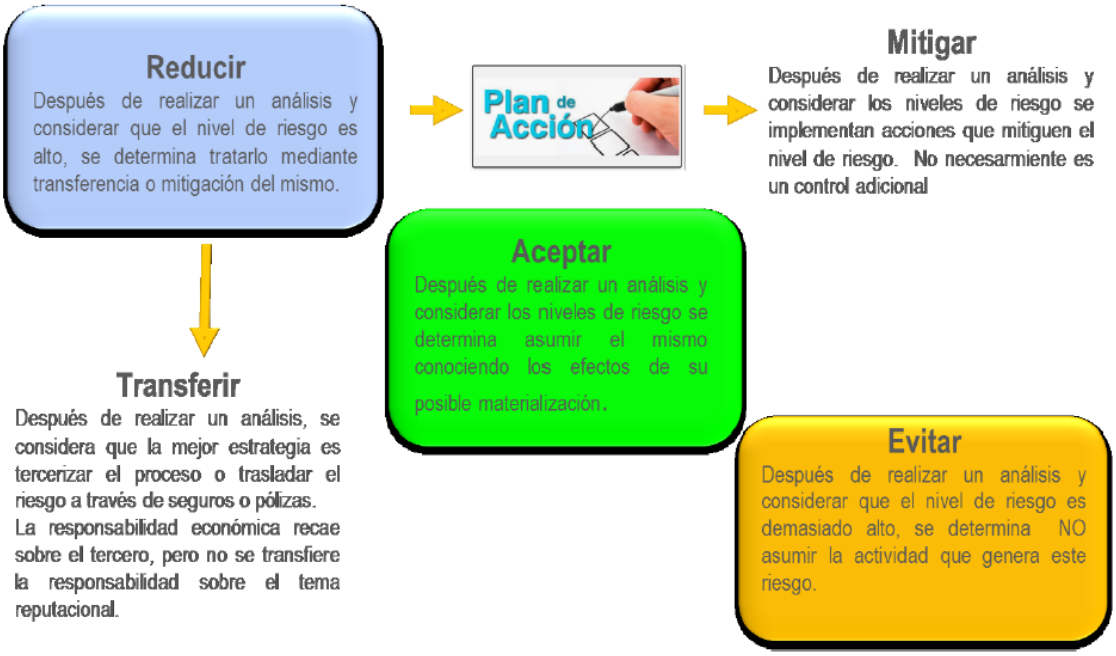
- Para mitigar/tratar los riesgos de seguridad de la información se deben emplear los controles del anexo A de la ISO/IEC 27001:2013 que apliquen.

7.2.2 Niveles para calificar el impacto

Para el establecimiento de la probabilidad de ocurrencia del riesgo y el nivel de consecuencia o impacto, con el fin de estimar la zona de riesgo inicial (riesgo inherente) se utilizará la **Tabla de Probabilidad** y la **Tabla de Impacto** establecidas en *la Guía para la administración del riesgo y el diseño de controles en entidades públicas* del DAFP 2022, las cuales están incorporadas en la herramienta de Excel puesta a disposición por el Departamento Administrativo de la Función Pública – DAFP y que fue adaptada para la gestión y administración de riesgos en la Empresa.

7.2.3 Tratamiento de riesgos

La empresa adopta las ***estrategias para combatir el riesgo***, entendidas como decisiones que se tomen frente a un determinado nivel de riesgo. Según la *Guía para la administración del riesgo y el diseño de controles en entidades públicas* del DAFP 2022, existen tres opciones y es importante mencionar, que las decisiones se deben tomar realizando un análisis frente al riesgo residual, esto para procesos en funcionamiento, y cuando se trate de procesos nuevos, se procede a partir del riesgo inherente.



Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2022.

7.2.4 Periodicidad para la revisión, el seguimiento, el monitoreo y la evaluación de los riesgos

La revisión, seguimiento, monitoreo y evaluación de los riesgos se realizará de la siguiente manera, de acuerdo con el nivel de riesgo residual:

7.2.4.1 Revisión

Los Líderes de Proceso revisarán completamente el mapa de riesgos, mínimo una vez al año, y para ello tomarán como insumo:

a. El contexto de la empresa.
b. Los resultados de las auditorías realizadas por la Oficina de Control Interno y Organismos de Control.
c. Lo reportado en los Comités de Autoevaluación y Seguimiento en relación a la administración de riesgos, establecido en la Circular 009 de 2017.
d. La materialización de los riesgos u ocurrencia de incidentes que afecten el logro de los propósitos y metas institucionales.
e. Informes de evaluación independiente del Sistema de Administración de Riesgos de la Empresa.

f. Las novedades o recomendaciones del Comité Institucional de Coordinación de Control Interno.
g. Los informes de monitoreo.

Esta revisión será realizada por el Líder de Proceso y su equipo de trabajo, y si lo requiere, con el acompañamiento de la Oficina Asesora de Planeación, la Subgerencia de Gestión Corporativa y/o la Oficina de Control Interno. El control de cambios del Mapa de Riesgos Institucional estará bajo la responsabilidad de la Oficina Asesora de Planeación.

7.2.4.2 Seguimiento

Los Líderes de Proceso deben realizar cuatrimestralmente el seguimiento al Mapa de Riesgos Institucional y entregar el informe con los resultados obtenidos, dentro de los 5 primeros días hábiles posteriores al cierre, a la Oficina de Control Interno; el cual incluirá el análisis de los riesgos y los controles para determinar si requiere de algún ajuste.

7.2.4.3 Monitoreo

- La Oficina Asesora de Planeación cuatrimestralmente elaborará los informes de monitoreo a los riesgos de corrupción, como Segunda Línea de Defensa y los socializará a los Líderes de Proceso para la toma de acciones.

- Cuando se detecte la materialización de un riesgo, los Líderes de Proceso deben hacer monitoreo en las fechas establecidas en el Plan de Mejoramiento y en los Planes de Contingencia respectivos. Para ampliar la información frente a la materialización de los riesgos ver numeral 7.5.

7.2.4.4 Evaluación

La Oficina de Control Interno evaluará cuatrimestralmente (30 de abril, 31 de agosto y 31 de diciembre) de cada vigencia en forma independiente el proceso de administración de los riesgos de la empresa y presentará semestralmente al Comité Institucional de Coordinación de Control Interno el informe correspondiente, con el fin de evidenciar si se materializó algún riesgo, si es necesario actualizar los mapas de riesgos o si se requiere eliminar alguno que con el tiempo no aplique a la Empresa. Lo anterior, en armonía con el seguimiento a los riesgos de corrupción y al Programa de Transparencia y Ética Pública.

De otra parte, la Oficina de Control Interno como Tercera Línea de Defensa, a través de sus procesos de seguimiento y evaluación, especialmente a través de la auditoría interna,

se pronunciará sobre la eficacia de las acciones para abordar riesgos y oportunidades y la efectividad de los controles para evitar la materialización de los riesgos. Para ampliar información respecto de la evaluación de la efectividad de los controles, ver numeral 7.4.4 Tercera Línea de Defensa.

Nota: Es de anotar que, aunque la Oficina de Control Interno se pronuncie frente a la efectividad de los controles, esto no es un indicativo de que con ello se evite la materialización del riesgo.

7.3 MATERIALIZACIÓN DE RIESGOS

Teniendo en cuenta que siempre existe la probabilidad de que un riesgo se materialice o se presente un incidente, a continuación, se dan unas pautas para definir el proceder ante esta eventualidad.

7.3.1 Definición del mapa de riesgos

Durante la definición de la matriz de riesgos de cada proceso o del documento que identifique riesgos (cuando se trate de proyectos o programas), el Líder de Proceso y/o responsables definidos deben definir acciones de contingencia para sus riesgos residuales con el fin de determinar cómo se debe actuar en caso de su materialización.

7.3.2 Materialización de riesgos

Cuando se materialice un riesgo (esté o no identificado en la Matriz de Riesgos Institucional o en el documento que identifique riesgos, cuando se trate de proyectos o programas), de forma inmediata, el Líder de Proceso debe:

a. Informar sobre la materialización del riesgo a las instancias de control internas y externas correspondientes con el tipo de riesgo.

b. Reportar a la Oficina Asesora de Planeación, a través del formulario disponible en la intranet para tal fin.

c. Implementar las acciones de contingencia correspondientes, ante la materialización de los riesgos que impliquen la interrupción de las operaciones.

d. Definir el Plan de Mejoramiento de acuerdo con lo establecido por el proceso *Evaluación y Seguimiento*.

e. Agendar una sesión de trabajo con la Oficina Asesora de Planeación, si lo considera necesario, para recibir asesoría metodológica para validar las causas de la materialización, efectividad de los controles y acciones de contingencia, para actualizar la matriz de riesgos (que trasciende a incluir el riesgo materializado que no estaba descrito en la matriz -cuando aplique-).
Nota: Para el caso de los riesgos de proyectos, se recomienda priorizar la asesoría metodológica para aquellos riesgos que se encuentren en la clasificación de alto y extremo (o calificaciones más altas de acuerdo con la estimación de la matriz de probabilidad e impacto del proyecto en particular).

7.4 NIVELES DE RESPONSABILIDAD SOBRE LA GESTIÓN Y ADMINISTRACIÓN DEL RIESGO

Además de las responsabilidades establecidas en la sección *7.2.4 Periodicidad para la revisión, el seguimiento, el monitoreo y la evaluación de los riesgos*, a continuación, se definen las siguientes por Línea de Defensa:

7.4.1 Línea de Defensa Estratégica

Responsables: Alta Dirección y Comité Institucional de Coordinación de Control Interno.

Responsabilidad frente al riesgo:

- Establecer y aprobar la Política para la Administración de Riesgos.
- Definir el marco general para la gestión del riesgo y el control y supervisar su cumplimiento.
- Realizar seguimiento y análisis periódico a los riesgos, y emitir instrucciones sobre las acciones apropiadas para la mejora, cuando aplique.
- Revisar los cambios en el direccionamiento estratégico y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados.
- Determinar los ajustes necesarios que se deban hacer frente a la gestión del riesgo.
- Solicitar las intervenciones e informes necesarios a las diferentes dependencias con el fin de facilitar la toma de decisiones.
- Evaluar el estado del sistema de control interno y aprobar las modificaciones, actualizaciones y acciones para su fortalecimiento.

7.4.2 Primera Línea de Defensa

Responsables: Líderes o responsables de los procesos.

Responsabilidad frente al riesgo:

- Identificar y valorar los riesgos que pueden afectar los procesos, proyectos o programas a su cargo y diseñar, implementar y monitorear los controles que permitan gestionar de manera directa los riesgos.
- Identificar riesgos de servicios o actividades tercerizadas.
- Revisar el mapa de riesgos por lo menos una vez en el año y actualizarlo si se requiere, y una vez aprobado por el líder del proceso, enviarlo a través de correo institucional a la Oficina Asesora de Planeación para su publicación en la intranet y página web, cuando se trate de riesgos asociados a los procesos.
- Socializar al interior del equipo de trabajo el mapa de riesgos y sus controles.
- Revisar y evaluar la ejecución de los controles aplicados por el equipo de trabajo en la gestión del día a día, detectar las deficiencias de los controles y determinar las acciones de mejora a que haya lugar.
- Reportar cualquier novedad sobre los riesgos a la Oficina de Control Interno y al Comité Institucional de Coordinación de Control Interno.
- Entregar cuatrimestralmente a la Oficina de Control Interno (Tercera Línea de Defensa) el informe con los resultados del seguimiento, el cual incluirá el análisis de los riesgos y los controles para determinar si requiere de algún ajuste.
- Dar a conocer a la Oficina Asesora de Planeación las apreciaciones y propuestas sobre los Riesgos de Corrupción que funcionarios y contratistas formulen, para su análisis e incorporación en caso de ser procedentes.
- Revisar que las actividades de control de sus procesos se encuentren documentadas y actualizadas en los procedimientos.
- Proponer mejoras a la gestión del riesgo de su proceso, proyecto o programa.
- Revisar y analizar los informes de evaluación y auditoría en materia de riesgos, y tomar las acciones necesarias que correspondan.
- En caso de materialización de riesgos se debe proceder con lo establecido en la sección **7.3 Materialización de riesgos**. De igual manera, ante la materialización de los riesgos que impliquen la interrupción de las operaciones se deben implementar los planes de contingencia correspondientes.
- Identificar cambios que podrían tener impacto significativo en el Sistema de Control Interno que se identifiquen durante evaluaciones periódicas de riesgos y en los trabajos de auditoría interna.

7.4.3 Segunda Línea de Defensa

Responsables: Oficina Asesora de Planeación – Líderes de la implementación de las Políticas establecidas en el Modelo Integrado de Planeación y Gestión -MIPG – Líderes o Coordinadores de otros sistemas de gestión, Coordinadores de equipos de trabajo, Directores de Contratación, Financiera y de TIC de la Empresa.

Responsabilidad frente al riesgo:

- Asesorar a la Línea Estratégica en la definición de la Política para la Administración de Riesgos, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo.
- Acompañar, orientar y entrenar a los líderes de procesos en la identificación, análisis y valoración del riesgo y definición de controles en los temas a su cargo.
- Revisar el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la Primera Línea de Defensa y determinar las recomendaciones y seguimiento para el fortalecimiento de éstos.
- Monitorear los riesgos identificados y los controles establecidos por la Primera Línea de Defensa acorde con la información suministrada por los Líderes de Proceso y con la estructura de los temas a su cargo.
- Evaluar la coherencia de los riesgos con la presente política y verificar que sean monitoreados por la Primera Línea de Defensa.
- Proponer las acciones de mejora a que haya lugar.
- Identificar cambios que podrían tener impacto significativo en el Sistema de Control Interno que se identifiquen durante evaluaciones periódicas de riesgos y en los trabajos de auditoría interna.

7.4.4 Tercera Línea de Defensa

Responsable: Oficina de Control Interno.

Responsabilidad frente al riesgo:

- Proporcionar una evaluación objetiva y razonable sobre las acciones para abordar riesgos y oportunidades y la efectividad de la gestión del riesgo y control en todas sus etapas, con énfasis en el diseño e idoneidad de los controles establecidos en los procesos.
- Asesorar y acompañar de forma coordinada con la Oficina Asesora de Planeación, y la Subgerencia de Gestión Corporativa, a la Primera Línea de Defensa acerca de las

metodologías, herramientas y técnicas para la identificación y administración de los riesgos y controles.

- Evaluar que se hayan identificado los riesgos significativos que afectan en el cumplimiento de los objetivos de los procesos, incluyendo los riesgos de corrupción y fraude.
- Evaluar el adecuado diseño y ejecución de los controles para la mitigación de los riesgos que se han establecido por parte de la Primera Línea de Defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de los mismos.
- Llevar a cabo la evaluación independiente de la gestión de los riesgos de conformidad con el Plan Anual de Auditoría y reportar los resultados al Comité Institucional de Coordinación de Control Interno y publicarlos en la página web de la Empresa.
- Recomendar mejoras a la Política de Administración del Riesgo.
- Identificar y evaluar cambios que podrían tener impacto significativo en el Sistema de Control Interno que se identifiquen durante evaluaciones periódicas de riesgos y en los trabajos de auditoría interna.
- Evaluar los cambios en el direccionamiento estratégico o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de que se identifiquen y actualicen las matrices de riesgos por parte de los responsables.
- Promover ejercicios de autocontrol para que cada proceso monitoree los niveles de eficiencia, eficacia y efectividad de los controles.
- Evaluar cuatrimestralmente el adecuado diseño y ejecución de los controles para la mitigación de los riesgos definidos en la matriz institucional, que se han establecido por parte de la Primera Línea de Defensa y realizar las recomendaciones y seguimiento para su fortalecimiento.
- Evaluar de manera independiente la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar.
- Evaluar el perfil de riesgo inherente y residual por cada proceso consolidado y pronunciarse sobre cualquier riesgo que esté por fuera del perfil de riesgo de la empresa o que su calificación del impacto o probabilidad del riesgo no es coherente con los resultados de las auditorías realizadas.

7.5 OTROS LINEAMIENTOS O POLÍTICAS DE OPERACIÓN

7.5.1 Lineamientos SARLAFT

Para la administración de los riesgos de Lavado de Activos y Financiación del Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva LA/FT/FPADM, es necesario tener en cuenta los siguientes principios:

Protección de la información: Los colaboradores de RenoBo son la garantía ante eventuales situaciones de riesgo de Lavado de Activos y Financiación del Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva. Todos los colaboradores actuarán con la mayor diligencia posible para proteger los recursos financieros de la Empresa, así como la información y los bienes.

Integridad y respeto: La integridad y el respeto como conductas, implican el acatamiento a las normas relacionadas con el control y prevención del Lavado de Activos y Financiación del Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva y del cumplimiento de las normas internas que RenoBo disponga para ello. Igualmente, se espera de los colaboradores un comportamiento dentro de los más altos estándares éticos y morales, de acuerdo con las directrices definidas en el Código de Integridad y en la *Política operativa de Integridad, Conflicto de Intereses y Gestión Anti soborno* (PL-07).

En ese sentido, para la administración de los riesgos de Lavado de Activos y Financiación del Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva LA/FT/FPADM, se imparten los siguientes lineamientos:

- RenoBo reconoce que el Lavado de Activos y Financiación del Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva significan un alto riesgo para la economía, la seguridad de la ciudad y el país y afecta directamente la transparencia, confianza, eficacia y la reputación en los procesos de la Empresa.
- RenoBo acatará las normas existentes y que se generen al interior de la Empresa en materia de prevención del Lavado de Activos y Financiación del Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva, con el propósito no sólo de contribuir a la realización de los fines del Estado y de cumplir la Ley, sino de proteger la imagen y la gestión institucional.
- RenoBo cumplirá con las directrices emitidas por su Junta Directiva y órganos de control sobre la Prevención y el Control del Lavado de Activos y Financiación del Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva.

- RenoBo divulgará la Política operativa de Integridad, Conflicto de Intereses y Gestión Anti soborno (PL-07), el Código de Integridad y Código de Buen Gobierno creado para asegurar un comportamiento ético y moral de sus colaboradores y mantendrá un programa permanente de capacitación sobre dicha materia.
- Cuando se requiera, RenoBo solicitará de sus clientes la confirmación de que sus operaciones cumplen con las normas y estándares de Prevención y Control del Lavado de Activos y Financiación del Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva.
- RenoBo analizará y verificará que la información entregada por sus proveedores cumple con la norma sobre Prevención y Control del Lavado de Activos y Financiación del Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva.
- RenoBo verificará la información de sus colaboradores y proveedores, y adelantará las campañas preventivas necesarias para concientizarlos sobre la importancia del cumplimiento de los valores consagrados en el Código de Integridad.
- RenoBo colaborará con las autoridades en proveer la información que sea solicitada en el desarrollo de procesos de investigaciones de Lavado de Activos y Financiación del Terrorismo y Financiamiento de la Proliferación de Armas de Destrucción Masiva.

7.5.2 Lineamientos generales

- La Oficina Asesora de Planeación, en coordinación y apoyo de la Oficina de Control Interno y la Subgerencia de Gestión Corporativa, deberán realizar, al menos una vez al año, actividades de capacitación y divulgación a todos los colaboradores de la empresa en gestión del riesgo para fortalecer la cultura de prevención y control. Es importante señalar, que el rol de la Oficina de Control Interno es de asesoría, lo que no afecta el proceso de evaluación independiente que se hace periódicamente sobre el tema.

- La actualización de los riesgos se debe realizar de manera permanente dado su naturaleza, los cambios en el contexto, materialización de los riesgos, actividades de comunicación y consulta, el seguimiento realizado por el Líder del Proceso o responsables definidos, el ejercicio de monitoreo, cambios en el proceso, proyecto o programa entre otros, por lo cual es importante que como mínimo éstos sean revisados al menos una vez en cada vigencia, y en caso de ser oportuno, actualizados, así:

    - **Riesgos de corrupción**: En diciembre de cada vigencia, para su oportuna socialización y posterior seguimiento y monitoreo.

- **Riesgos de gestión**: En el primer trimestre de cada vigencia, permitiendo así su oportuna socialización a los interesados y realizar respectivamente sus seguimientos y monitoreos.
- **Riesgos de seguridad de la información**: En el tercer trimestre de cada vigencia, permitiendo así su oportuna socialización a los interesados y realizar respectivamente sus seguimientos y monitoreos.
- **Riesgos de seguridad y salud en el trabajo**: En el cuarto trimestre de cada vigencia, pero hay casos especiales en los que deberá actualizar, como: accidentes de trabajo mortales, eventos catastróficos dentro de la compañía o cuando hay cambios en los procesos.
- **Riesgos ambientales (Aspectos e Impactos)**: La matriz de aspectos e impactos ambientales deberá ser actualizada y reportada en los siguientes casos:
  - Cuando se rediseña el proceso de Gestión Ambiental.
  - Cuando se cambia el alcance del proceso de Gestión Ambiental (nueva sede, nuevos procesos, nuevos productos).
  - Cuando se presenten nuevos desarrollos de productos o servicios.
  - En los términos establecidos por la Autoridad Ambiental, una vez al año.
- **Riesgos de proyectos**: para los proyectos mayores a un año se deberá hacer como mínimo una revisión anual; no obstante, cada vez que se actualicen parámetros del proyecto, se materialice un riesgo, se presenten cambios en los recursos, metas, entregables, haya afectación por factores externos o a discreción de los equipos de proyectos.

- Para el caso de riesgos de procesos, los Líderes de Proceso son los encargados de aprobar las actualizaciones de los mapas de riesgos y de enviarlos a través de correo institucional a la Oficina Asesora de Planeación para su consolidación y su publicación en la intranet y en la página web de la empresa. En caso de presentarse eliminaciones de riesgos, se debe enviar la respectiva justificación. Para el caso riesgos de proyectos o programas, las Subgerencias o líderes de proyectos son los encargados de aprobar las actualizaciones de las matrices o registro de riesgos y podrán solicitar apoyo metodológico a la Oficina Asesora de Planeación para tal fin, en todo caso se deberá compartir la información actualizada con la Oficina Asesora de Planeación para su consolidación.

- Al identificar riesgos para cada uno de los procesos, proyectos o programas, es importante establecer su relación con el cumplimiento de la estrategia organizacional, para garantizar una alineación con el marco estratégico institucional.

- Los riesgos de seguridad de la información se deben gestionar de acuerdo con los criterios diferenciales descritos en el Modelo de Seguridad y Privacidad de la Información de la empresa.

Política para la Administración de Riesgos

- Se deben identificar riesgos de corrupción en trámites y otros procedimientos administrativos – OPA, de acuerdo con los lineamientos dados por el Departamento Administrativo de la Función Pública y por la Secretaría General de la Alcaldía Mayor de Bogotá.

- La Oficina Asesora de Planeación deberá consolidar y publicar el Mapa de Riesgos por procesos en la intranet y en la página web de la empresa a más tardar el 31 de enero de cada vigencia, para dar cumplimiento a lo establecido en el literal g del artículo 9 de la Ley 1712 de 2014 y el artículo 31 de la Ley 2195 de 2022.

- Para mitigar/tratar los riesgos de seguridad de la información se deben emplear los controles del anexo A de la ISO/IEC 27001:2013 que apliquen.

- Los Líderes de Proceso podrán solicitar asesoría a la Oficina Asesora de Planeación, a la Subgerencia de Gestión Corporativa o a la Oficina de Control Interno para la formulación o actualización de los Mapas de riesgos.

- Los eventos de corrupción realizados por servidores y ex servidores de la empresa serán investigados por la Oficina de Control Disciplinario Interno con el fin de establecer las responsabilidades a que haya lugar, tomar las medidas administrativas pertinentes y adelantar las denuncias correspondientes. De acuerdo con lo previsto en el artículo 70 de Ley 1952 de 2019, los contratistas sólo serán disciplinables si cumplen función pública, y será competente para adelantar las respectivas investigaciones, la Procuraduría General de la Nación.

- RenoBo pone a disposición de sus colaboradores y de terceros, todos los canales de comunicación que permitirán obtener información sobre la potencial ocurrencia de prácticas de corrupción, internas o externas y de manera especial, en la página web de la Empresa se dispone del botón visible para que colaboradores, ciudadanos y terceros puedan presentar las denuncias por posibles actos de corrupción, existencia de inhabilidades, incompatibilidades o conflicto de intereses. De igual manera, en cumplimiento del principio de armonización de canales, la Secretaría General de la Alcaldía Mayor de Bogotá, D. C., pone a disposición los siguientes canales:

    - <u>Presencial</u>
        - ✓ Punto de atención a la ciudadanía RenoBo Autopista Norte No. 97-70 piso 3, Buzón de sugerencias
        - ✓ A nivel Distrital: SuperCADE y CADE
        - ✓ Super CADE MOVIL

- ✓ Puntos de Atención a la ciudadanía de las entidades Distritales
- ✓ Escrito: De manera física en las oficinas de correspondencia de las entidades distritales.

- Virtual
  - ✓ SuperCADE Virtual
  - ✓ En RenoBo: correo electrónico atencionalciudadano@renobo.com.co y defensordelciudadano@renobo.com.co, redes sociales
  - ✓ Sistema Distrital para la Gestión de Peticiones Ciudadanas – "Bogotá te escucha"; a través de la ruta https://bogota.gov.co/sdqs/denuncias-por-actos-de-corrupcion

- Telefónico
  - ✓ En RenoBo Línea fija 3599494 Ext. 500
  - ✓ A nivel Distrital: Línea 195; por este canal los usuarios tienen la posibilidad de presentar denuncias, y obtener orientación personalizada frente a sus casos, con el fin de registrar y direccionar adecuadamente las solicitudes.

- Todo colaborador de la empresa está obligado a comunicar a través de cualquiera de los canales de comunicación, todo acto irregular de otro colaborador o tercero, que afecte o pueda lesionar los intereses de la empresa, así como cualquier acto de corrupción.

- Las denuncias o quejas sobre actos de corrupción que se reciban por cualquier canal de comunicación se deberán remitir al Defensor del Ciudadano y a la Oficina de Control Disciplinario Interno.

- El Jefe de la Oficina de Control Disciplinario Interno es el responsable de consolidar y generar los informes de gestión semestrales sobre denuncias o quejas sobre actos de corrupción que se reciban para presentarlos a la Gerencia General.

- La empresa no tomará represalias contra los colaboradores y terceros que denuncien hechos sospechosos y mantendrá su confidencialidad, con el fin de proteger su identidad e integridad.

8. EVALUACIÓN DE LA POLÍTICA

De acuerdo con lo establecido en la Resolución 195 de 2018 "*Por la cual se crea y se reglamenta el funcionamiento del Comité Institucional de Coordinación de Control Interno de la Empresa de Renovación y Desarrollo Urbano de Bogotá D.C.*", el Comité

Institucional de Coordinación de Control Interno realizará seguimiento a la implementación de esta Política, en especial, a la prevención y detección de fraude y mala conducta.

De otra parte, y según lo establecido en la sección *7.2.4 Periodicidad para la revisión, el seguimiento, el monitoreo y la evaluación de los riesgos*, a continuación, se resaltan los mecanismos a través de los cuales se realizará evaluación al cumplimiento de la presente Política:

- La Oficina Asesora de Planeación cuatrimestralmente elaborará los informes de monitoreo como Segunda Línea de Defensa y los socializará a los líderes de proceso para la toma de acciones.

- La Oficina de Control Interno evaluará cada 4 meses (30 de abril, 31 de agosto y 31 de diciembre) en cada vigencia en forma independiente el proceso de administración de los riesgos de la empresa y presentará el informe correspondiente al Comité Institucional de Coordinación de Control Interno, con el fin de evidenciar si se materializó algún riesgo, si es necesario actualizar los mapas de riesgos o si se requiere eliminar alguno que con el tiempo no aplique a la Empresa. Lo anterior en armonía con el seguimiento a los riesgos de corrupción y el Programa de Transparencia y Ética Pública.

Política para la Administración de Riesgos

CONTROL DE CAMBIOS

Versión	Fecha	Descripción de la modificación
1	14/12/2022	Documento original.
2	30/11/2023	Actualización del documento en los siguientes temas: detalle del compromiso de la alta dirección frente a los riesgos, detalle de las tipologías de riesgos a los cuales está expuesta la empresa, inclusión de lineamientos relacionados con SARLAFT y riesgos en proyectos que lidere la empresa. Política aprobada en el marco del Comité Institucional de Coordinación de Control Interno el 29 de noviembre del 2023.
3	08/11/2024	Actualización participativa de la política de acuerdo con la nueva estructura de la empresa, así como ajustes generales del documento para dar mayor claridad y mejorar su entendimiento e implementación. Política aprobada en el marco del Comité Institucional de Coordinación de Control Interno el 8 de noviembre del 2024.

REGISTRO DE FIRMAS ELECTRONICAS

PL-08_Pol_Admon_Riesgos_V3

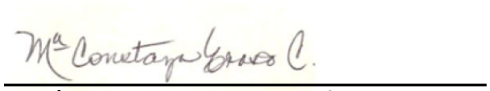
EMPRESA DE RENOVACIÓN Y DESARROLLO URBANO DE BOGOTÁ
gestionado por: azsign.com.co

Id Acuerdo: 20241108-154037-cb1af4-29122177
Estado: Finalizado

Creación: 2024-11-08 15:40:37
Finalización: 2024-11-08 15:42:00

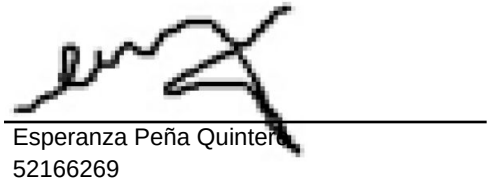
Escanee el código para verificación

Aprobación: Oficina Asesora de Planeación



María Constanza Eraso Concha
52054750
merasoc@renobo.com.co
Subgerente de Planeación y Administración de Proyectos
Empresa de Renovación y Desarrollo Urbano de Bogotá

Elaboración: Oficina Asesora de Planeación



Esperanza Peña Quintero
52166269
epenaq@renobo.com.co
Contratista
Empresa de Renovación y Desarrollo Urbano de Bogotá

REPORTE DE TRAZABILIDAD

PL-08_Pol_Admon_Riesgos_V3

EMPRESA DE RENOVACIÓN Y DESARROLLO URBANO DE BOGOTÁ
gestionado por: azsign.com.co

Id Acuerdo: 20241108-154037-cb1af4-29122177
Creación: 2024-11-08 15:40:37
Estado: Finalizado
Finalización: 2024-11-08 15:42:00

Escanee el código para verificación

TRAMITE	PARTICIPANTE	ESTADO	ENVIO, LECTURA Y RESPUESTA
Elaboración	Esperanza Peña Quintero epenaq@renobo.com.co Contratista Empresa de Renovación y Desarrollo Urban	Aprobado	Env.: 2024-11-08 15:40:38 Lec.: 2024-11-08 15:40:52 Res.: 2024-11-08 15:41:10 IP Res.: 181.63.25.26
Aprobación	María Constanza Eraso Concha merasoc@renobo.com.co Subgerente de Planeación y Administració Empresa de Renovación y Desarrollo Urban	Aprobado	Env.: 2024-11-08 15:41:10 Lec.: 2024-11-08 15:41:30 Res.: 2024-11-08 15:42:00 IP Res.: 181.51.197.222